Mark Chandler
Senior Vice President, General Counsel
Cisco Systems, Inc.
February 15, 2005
U.S. House of Representatives, Committee on International Relations

---

Mr. Chairman, Members of the Subcommittee:

My name is Mark Chandler, Senior Vice President and General Counsel of Cisco Systems. Thank you for the opportunity to address some very important and difficult issues. Cisco strongly supports free expression and open communication on the Internet, and we respect the strength of conviction of those who have brought these concerns forward.

The Committee is exploring the question of Chinese government censorship of the Internet. In this regard:

- Cisco does not customize, or develop specialized or unique filtering capabilities, in order to enable different regimes to block access to information
- Cisco sells the same equipment in China as it sells worldwide
- Cisco is not a service or content provider, or network manager
- Cisco has no access to information about individual users of the Internet

Cisco does, however, comply with all U.S. Government regulations which prohibit the sale of our products to certain destinations, or to certain users or to those who resell to prohibited users. We have not sold and do not sell our equipment to the countries listed on the U.S. Department of Treasury's OFAC (Office of Foreign Assets Control) list of embargoed nations, and we comply fully with all aspects of the Foreign Relations Authorization Act passed by Congress in the wake of the Tiananmen Square incident.

Cisco has played a leading role in helping to make Internet technology ubiquitous, allowing hundreds of millions of people in nearly every nation around the world to access information and ideas previously unavailable or inaccessible. Because our products are designed to expand the reach of communications systems, we build to open, global standards. We do not design custom or closed Internet systems. The Internet technology may not be perfect -- and the Internet itself can be misused -- but there has been no greater force in spreading the power of ideas than the single worldwide Internet. The key

to its growth and the flow of information it enables has been the standardization of one global network. This has been and remains the core of Cisco's mission.

Cisco was founded 22 years ago by two computer scientists at Stanford University who were seeking a way to exchange information between different computer systems in two different departments. At that time, such communication was very difficult if not impossible even within a college campus, although today it is, of course, common across the world. Our founders developed a device to communicate between their disparate computer systems. This became the first product of Cisco Systems, known as a router. Today we are a leading supplier of Internet equipment. We employ nearly 30,000 people in the United States and 10,000 overseas. We have annual sales of approximately $27 billion, and we hold over 2,000 issued US patents and have applied for over 3,000 more.

Networking equipment (routers and switches) forms the core of the global Internet and most corporate and government networks. Cisco makes the equipment that makes the Internet and networking work. We are often described as the "plumbers" of the Internet, as our technology constitutes the "pipes" that connect point A to point B. Originally our products were designed for communications within private or enterprise networks. When the public Internet emerged in the mid '90s, our products found immediate application for worldwide use. We now have many competitors around the world who build products that perform similar functions. When you send an email in your office to your children or grandchildren, the digital language that makes up that email is routed through equipment made by Cisco or our competitors.

Networks that existed in the early 1970s would eventually evolve into the Internet, but at the time Cisco was founded, the Internet as we know it today did not exist. As the Internet grew, it moved from societal novelty to a critical part of the communications infrastructure of our country and the world. It unfortunately also became the target of attacks, the intended result of which was to attempt to reduce its capability to operate by impeding or entirely preventing its ability to provide communications services to millions of users. These attacks can take many forms, some of which are referred to as worms, viruses, denial of service attacks, and more. Network management and security capabilities – including technology generically referred to as filtering -- are essential to mitigate attacks and thus enable information flow. No network can be administered without the ability to manage and protect the information that flows through it. Without this capability, it would not be possible to operate the Internet and the Internet would likely not exist as it does today.

The technology that is used to manage and protect against hackers or websites that host viruses is also the same generic technology that allows libraries and parents to filter or control internet access by children, such as via AOL's parental controls, or block pornography or the illegal downloading of copyrighted material. If, for example, a network administrator knows that a certain website is dangerous to her network because a virus or spyware has been downloaded from that site, or because the site is pornographic, she can use IP address blocking (each website and user on the Internet has an IP – Internet Protocol – address - the equivalent of a phone number) to protect her network

from that site. This technology is a customary part of network management software of all major suppliers of Internet equipment -- Cisco's and our competitors' -- and is basic to network functionality. Whether for security or the management of information, the technology is one and the same. The filtering that occurs is implemented by the owner or administrator of the network using technology that is available regardless of the manufacturer.

Some countries have chosen to restrict or limit access to information on the Internet based on political considerations, rather than on the freedoms that we enjoy in this country. While many have commented on the activities of the Chinese government in this regard, the issue is, in fact, global. Some Middle Eastern countries block sites critical of their leadership. And judicial action has been taken in France due to the failure of an operator to block French users' access to some types of information. Cisco however has not and does not design products to accommodate political censorship. The tools built into our products that enable site filtering are the same the world over, whether sold to governments, companies or network operators. The features in our equipment are "off the shelf" and not altered in any way for any market or region. Similar technology is available from at least a dozen other US, Canadian, European and Chinese companies. Because of threats to network operations, which exist around the world, there is no way to market equipment without these capabilities. The management of information flow by a customer cannot be prevented by Cisco unless we are to also prevent the originally intended use of this technology, which would expose the Internet to the full risks of inevitable daily attacks. Networks attached to the Internet would literally stop working.

Our innovative products have helped lead the world into the Internet age and are truly changing the way the world lives, works, learns and plays. For instance, since our entry into the Chinese market in 1994, the number of Chinese accessing the global Internet has grown from 80,000 in 1995 to over 130,000,000 in 2005 – a 1625% increase in the past 10 years. While Cisco certainly cannot take credit for all of the Internet growth in China, it shows that the appetite for information via the Internet is nearly impossible to contain. Is there any question that the Internet has provided to hundreds of millions of people access to information from around the world in a volume and with a speed unthinkable even a decade ago?

For some, the Internet is a tool that liberates individuals from the constraints of time and distance, empowering those who previously had no access to the world's store of information. Some are fearful of this liberation as they see the Internet as a mechanism for empowering non-state actors. Still others see the Internet as a tool used by governments to control content.

Any policy response to this divergence in views is necessarily complex. It must, however ensure the continuation of a single, worldwide Internet if the goal of global free expression is ever to be achieved. Among the questions most pertinent: Has the Internet helped spread a dramatic increase in access to information in regions where content is nonetheless subject to certain limitations? Does active engagement in such countries help to influence policy decisions? What policies will best help foster the ability to overcome

censorship? If countries that engage in censorship are to be denied US Internet technology, will those countries establish closed-standard Internets of their own to further restrict access to information? In our view, legislation or other action which encourages governments to build their own Internets will reduce free expression. Last year, the Chinese authorities proposed a special standard to allow Chinese companies alone to manufacture Internet equipment for China involving the use of encryption. Our government resisted that proposal, and we urge continued action in that regard. The power of the Internet to expand free expression depends on there being one global Internet. Efforts are underway, as illustrated in the attached article, to balkanize the Internet. Policies which promote that – even inadvertently – will undermine rather than support the many projects which help users evade censorship and will exacerbate rather than solve the problems we are discussing today.

The liberating power of the Internet depends on its existence as one global Internet. Its advent is a powerful force and its capabilities broad. Any policies in this area should, we believe, proceed from the realization that its very global nature provides a unique tool for the dissemination of ideas and cultivation of freedoms. We should do nothing to disturb its promise.

Thank you for inviting us to appear before you today.

END
